PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : **H04M 17/00, 17/02, G07F 7/10** — **A1**

(11) Numéro de publication internationale: **WO 99/49646**

(43) Date de publication internationale: 30 septembre 1999 (30.09.99)

(21) Numéro de la demande internationale: PCT/FR99/00292

(22) Date de dépôt international: 10 février 1999 (10.02.99)

(30) Données relatives à la priorité:
98/03483 20 mars 1998 (20.03.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: KOCH–HOURRIEZ, Carole–Audrey [FR/SG]; 11A Belmont Road, Singapore 269858 (SG). PAULIAC, Mireille [FR/FR]; Résidence Clair Soleil, Bâtiment B, Traverse des Aubes, F–13400 Aubagne (FR). BANCHELIN, Xavier [FR/FR]; 123, chemin des Amaryllis, F–13012 Marseille (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'activités de Gémenos, F–13881 Gémenos Cedex (FR).

(81) Etats désignés: AU, BR, CA, CN, IN, JP, KR, MX, RU, SG, US, VN, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

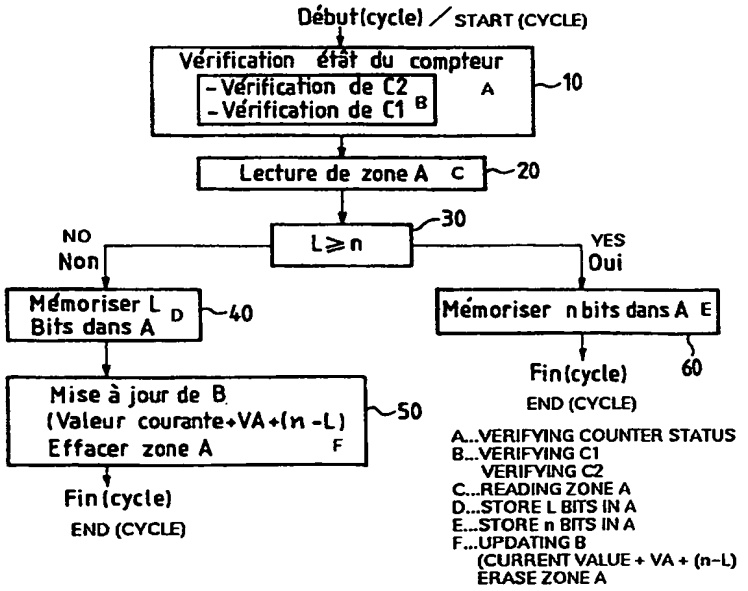
Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD FOR SECURELY MANAGING A UNITS COUNTER AND SECURITY MODULE IMPLEMENTING SAID METHOD

(54) Titre: PROCEDE DE GESTION SECURISEE D'UN COMPTEUR D'UNITES ET MODULE DE SECURITE METTANT EN OEUVRE LE PROCEDE

(57) Abstract

The invention concerns a method for securely managing a units counter in an electrically programmable and erasable memory, whereby a number of units consumed by users is recorded by means of a counter, consisting in breaking down the units counter into at least two memory zones (A, B), one first zone (A) wherein a bit is stored per unit consumed and a second zone (B) wherein the value corresponding to the accumulation of bits consumed is stored, the second zone being only updated when the number of units consumed exceeds or reaches the number of non–stored bits in the first zone. The invention is applicable to security modules provided in telephone terminals.



(57) Abrégé

L'invention concerne un procédé de gestion sécurisée d'un compteur d'unités dans une mémoire programmable et effaçable électriquement, selon lequel on enregistre un nombre d'unités consommées par des utilisateurs au moyen du compteur, consistant à décomposer le compteur d'unités en au moins deux zones mémoires (A, B), une première zone (A) dans laquelle on grille un bit par unité consommée et une deuxième zone (B) dans laquelle on mémorise la valeur correspondant au cumul d'unités consommées, la deuxième zone n'étant mise à jour que lorsque le nombre d'unités consommées dépasse ou atteint le nombre de bits non grillé dans la première zone. Application aux modules de sécurité placés dans des terminaux téléphoniques.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

PROCEDE DE GESTION SECURISEE D'UN COMPTEUR D'UNITES ET MODULE DE SECURITE METTANT EN OEUVRE LE PROCEDE

La présente invention a pour objet un procédé de gestion sécurisée d'un compteur d'unités implanté en mémoire, notamment d'une carte à puce en relation avec un terminal. Elle pourrait néanmoins s'appliquer à tout autre type de mémoire.

L'invention est particulièrement utile quand il s'agit de compter un très grand nombre d'unités tout en préservant la capacité de mémorisation de la mémoire.

De part la technologie employée par les fabricants de mémoire non volatiles effaçables et programmables électriquement (par exemple EEPROM), la faculté de mémorisation de la mémoire (aptitude à être mise à jour) est limitée dans le temps.

Les fabricants garantissent le bon comportement de la mémoire pour un nombre limité de mises à jour de la mémoire (une mise à jour comprend une opération d'effacement suivi d'une programmation ou écriture). Au delà, la mémoire risque de ne plus être effacée correctement ou être programmée correctement.

En moyenne, le nombre de mises à jour garanti par les fabricants de mémoire est de l'ordre de 100 000 par emplacement mémoire. Dans le cas d'un compteur d'unités, le problème consistant à préserver la faculté de mémorisation dudit compteur est d'autant plus difficile à résoudre que le nombre d'unités à compter est grand et que la fréquence de mise à jour du compteur est importante.

L'invention sera particulièrement décrite dans le cas d'une application à carte à puce dans le domaine de la publiphonie.

Il est connu dans le domaine de la carte à puce, qu'une transaction entre un terminal et un porte-

monnaie électronique externe est organisée autour d'un module de sécurité (MS) comprenant un microprocesseur. Le module est généralement intégré au terminal.

Le rôle d'un module de sécurité est notamment de veiller à la vérification de l'authentification des cartes porte-monnaie électroniques externes au terminal. Dans le cadre de la publiphonie, la carte à puce porte-monnaie est une télécarte (non rechargeable), le terminal est un publiphone (ou cabine téléphonique) et le module de sécurité peut être lui-même par exemple être une carte à puce implantée dans le terminal.

On peut noter que le jeu de commandes du composant dudit module de sécurité s'appelle "système d'exploitation".

L'utilisation d'un module de sécurité permet de donner à l'exploitant d'un publiphone les moyens d'authentifier les télécartes qui sont insérées par les clients porteurs desdites télécartes. Ainsi les cartes frauduleuses sont rejetées.

En plus des fonctions d'authentification, le module propose à l'exploitant d'un publiphone de gérer de manière sécurisée un compteur d'unités qui enregistre toutes les unités consommées par les différents titulaires de cartes à pré-paiement ou de télécartes durant les communications téléphoniques passées à partir dudit publiphone.

Cette fonctionnalité ouvre la voie à des solutions multi-opérateurs où l'émetteur des télécartes (opérateur) ne serait pas l'exploitant unique du publiphone. Pour cela, il est prévu de disposer au sein de la mémoire du module de sécurité implanté dans chaque publiphone, d'un compteur d'unités dédié à chaque opérateur.

Toujours dans le cadre de la publiphonie, un tel compteur doit pouvoir mémoriser plus de 16 millions d'unités ce qui correspond à un maximum d'unités téléphoniques susceptibles d'être enregistrées sur des lieux publics très fréquentés (aéroports) pour des mesures effectuées sur la durée de vie moyenne des compteurs d'un publiphone (environs 3 ans).

La mise à jour dudit compteur peut en outre être exigée à plusieurs reprises durant une communication téléphonique.

Pour mémoriser autant d'unités à l'aide des compteurs de l'art antérieur il faudrait utiliser une mémoire de 24 bits. Toutefois dans ce cas le nombre de mises à jour excéderait la capacité de mémorisation de cette mémoire. Cette solution n'est donc pas envisageable.

Dans l'invention, on a prévu de remédier à ce problème en décomposant le compteur d'unités en au moins deux zones principales.

La première zone mémoire du compteur (zone A) est considérée comme un champ de bits. A chaque bit mémorisé ou "grillé" ou "écrit" ou "allumé" correspond une unité de communication consommée. On parle également de "jeton" pour caractériser un bit mémorisé de la zone A.

Une seconde zone mémoire (zone B) plus restreinte dont la taille permet de coder la valeur maximale du nombre d'unités à mémoriser.

Ces zones mémoires sont des zones mémoire d'une mémoire non volatile programmable électriquement et effaçable électriquement.

S'agissant de la zone A et sans rentrer dans la technologie de programmation des mémoires, un emplacement mémoire sera considéré indisponible lorsque

un bit y sera mémorisé. On parlera dans la suite de manière indifférente de bit mémorisé ou de "bit allumé" ou de "bit grillé" ou de bit écrit pour signifier que les emplacements mémoire sont indisponibles et de bit éteint ou non grillés pour signifier que les emplacements sont disponibles (libres).

Par convention, on considérera qu'un bit est allumé lorsque son état logique est égal à 1, et qu'un bit est éteint lorsque son état logique est égal à 0.

Un bit allumé ne sera rendu disponible (éteint) qu'au prochain effacement de toute la zone A (extinction de tous les bits la composant).

L'invention a donc plus particulièrement pour objet un procédé de gestion sécurisée d'un compteur d'unités dans une mémoire programmable électriquement, selon lequel on enregistre un nombre d'unités consommées par des utilisateurs au moyen du compteur, principalement caractérisé en ce qu'il consiste à décomposer le compteur d'unités en au moins deux zones mémoires (A, B), une première zone (A) dans laquelle on mémorise au moins un bit par au moins une unité consommée et une deuxième zone (B) dans laquelle on mémorise la valeur correspondant au cumul d'unités consommées, la deuxième zone n'étant mise à jour que lorsque le nombre d'unités consommées dépasse ou atteint le nombre de bit non mémorisé de la première zone.

Les unités consommées sont enregistrées dans la première zone de manière cyclique.

Un cycle correspond à une séquence d'allumage du premier bit de la première zone (A) vers le dernier. Il prend fin lorsque tous les bits ont été allumés.

Une opération d'enregistrement de n unités consommées comprend les étapes suivantes :

- lecture du contenu de la première zone et comparaison du nombre de bits non mémorisés au nombre d'unités consommées à enregistrer,

- si ce nombre de bits non mémorisés est supérieur ou égal au nombre d'unités à enregistrer, on mémorise les bits à enregistrer dans ladite zone,

- si ce nombre est inférieur, on mémorise ce nombre de bits dans la première zone et on enregistre les unités restantes dans la deuxième zone en effectuant une opération de mise à jour de cette zone et la première zone est effacée.

Une opération de mise à jour de la deuxième zone (B) comprend une étape d'écriture dans cette zone d'une nouvelle valeur de compteur codée égale à la valeur courante à laquelle on ajoute le nombre de bits grillés de la première zone (A) et les unités restantes consommées à mémoriser.

La mise à jour de la deuxième zone comprend une étape préalable d'enregistrement d'une information témoin signifiant qu'une mise à jour est en cours, puis lorsque la mise à jour est terminée, la mise à jour consiste à effacer la première zone (A) et à effacer l'information témoin.

Pour améliorer la sécurité le compteur d'unité comporte une zone de sauvegarde (SB) de la deuxième zone (B) et ces deux zones comportent chacune un champs pour l'enregistrement d'un code de redondance (CR, SCR) pour la vérification de l'intégrité du contenu de ces deux zones.

Une opération d'enregistrement de n unités consommées comprend en outre une étape préalable de vérification de l'état du compteur comprenant les opérations suivantes :

- vérification de l'absence de l'information témoin d'une mise à jour en cours :

- dans le cas où l'information témoin est bien absente :

- vérification de la validité des champs contenant les codes de redondances :

. dans le cas où les champs sont valides :

- enregistrement des n unités;

. dans le cas où les champs ne sont pas valides :

- détection d'un défaut et arrêt du compteur,.

- dans le cas où l'information témoin est présente :

- activation de l'opération de recouvrement pour rétablir l'intégrité des contenus du compteur.

Une opération de mise à jour de la deuxième zone comporte alors les étapes suivantes:

- enregistrement de l'information témoin,
- recopie dans la zone de sauvegarde (SB) de la valeur du compteur codée de la deuxième zone (B),
- enregistrement de la nouvelle valeur du compteur codée dans la deuxième zone (B),
- effacement de la première zone (A),
- effacement de l'information témoin.

L'opération de recouvrement consiste à déterminer à quelle étape s'est produite l'anomalie (une coupure de courant), puis à opérer selon le cas déterminé, les étapes de mise à jour de la zone de sauvegarde (SB) et/ou de la deuxième zone (B) et/ou de la première zone.

Avantageusement, la détermination de l'étape à laquelle s'est produite l'anomalie consiste à lire le contenu de chacune des zones pour savoir si l'anomalie

s'est produite pendant la mise à jour de la zone de sauvegarde (SB) cas 1, pendant la mise à jour de la deuxième zone (B) cas 2, pendant l'effacement de la première zone (A) cas 3, entre la mise à jour de la deuxième zone (B) et la zone de sauvegarde (SB) cas 4, après la mise à jour de ces deux zones cas 5.

De façon pratique, le recouvrement consiste dans le cas 1 à :

- recopier la valeur contenue dans la deuxième zone (B) dans la zone de sauvegarde (SB),
- mettre à jour la deuxième zone (B) en enregistrant la nouvelle valeur qui est égale à l'ancienne à laquelle on ajoute le contenu de la première zone (A),
- effacer la première zone (A),
- effacer l'information témoin (C2) ;

dans le cas 2 à :

- recopier dans la deuxième zone (B) la valeur contenue dans la zone de sauvegarde (SB) en rajoutant la valeur contenue dans la première zone (A),
- effacer la première zone (A),
- effacer l'information témoin (C2) ;

dans le cas 3 à :

- effacer le contenu de la première zone (A),
- effacer l'information témoin (C2) ;

dans le cas 4 à :

- mettre en oeuvre les étapes selon le cas 2 ;

dans le cas 5 à :

- mettre en oeuvre les étapes selon le cas 3.

Avantageusement le procédé comprend en outre une étape d'enregistrement d'une information significative d'une défaillance en lecture ou en écriture de la première zone (A) désactivant ladite zone lorsqu'il n'a pas été possible de lire ou d'écrire dans cette zone,

et une étape de lecture de cette information à chaque nouveau cycle, les unités consommées étant alors directement enregistrées de manière codée par une opération de mise à jour de la deuxième zone (B).

L'information témoin (C2) d'une mise à jour en cours et l'information significative d'une défaillance (C1) en lecture et en écriture de la première zone sont enregistrées dans une troisième zone (C) dudit compteur.

L'invention concerne également un module de sécurité mettant en oeuvre le procédé conforme à l'invention.

Un tel module pourra être implanté dans un terminal gérant des unités consommées par les utilisateur du terminal, il pourra s'agir notamment d'un terminal de téléphonie.

D'autres particularités et avantages de l'invention apparaîtront à la lecture de la description qui est faite ci-après et qui est donnée à titre d'exemple non limitatif en regard des dessins annexés sur lesquels:

- la figure 1, représente de façon schématique le compteur d'unités selon l'invention ;
- la figure 2A, représente les étapes d'enregistrement de n unités selon le procédé de l'invention ;
- la figure 2B, représente l'étape préalable de vérification 10 de la figure 2A;
- la figure 3, représente les étapes d'enregistrement des unités dans la deuxième zone (mise à jour) selon un mode préféré de réalisation ;
- la figure 4, représente les étapes du mécanisme de recouvrement ;
- la figure 5, illustre une variante dans le procédé conforme à l'invention.

Le procédé décrit dans la suite concerne un compteur protégé contre la fraude (l'intrusion, la falsification). Le procédé prévoit que lorsque le compteur est saturé, ce dernier s'arrête et en informe l'application qui l'utilise.

Dans l'exemple d'application qui est donné ci-après, et qui correspond au cas de la publiphonie cité dans le préambule, les unités consommées sont des unités téléphoniques et les tailles des zones A et B sont bien évidemment définies ici à des fins d'exemple.

Il est pertinent de considérer une zone A de 168 bits et une zone B de 24 bits (24 bits permettent en effet de mémoriser 16 777 215 unités).

La zone B est à son tour dédoublée pour pallier à des problèmes de coupure de courant durant la mise à jour du compteur (cf. figure 1). Ce cas est détaillé dans la suite.

Comme cela a déjà été mentionné la durée d'exploitation du compteur est directement liée au nombre de mises à jour (effacement et écriture). Il est donc impératif de trouver une structure de compteur et un procédé de comptabilisation qui réduise le nombre de mises à jour.

Dans le cadre de l'invention, la mémorisation des unités de communication consommées s'effectue comme suit.

On suppose que la durée d'une communication téléphonique est divisée en plages de temps. La durée d'une plage de temps correspond à un nombre d'unités consommées fixé. Dans cet exemple, le cycle d'enregistrement des unités consommées sont définis par ces plages de temps.

Au début de chaque plage de temps, le nombre d'unités consommées doit être mémorisé dans le module de sécurité.

Ainsi, dans le cas d'une communication nécessitant 13 unités au total et où une plage de temps élémentaire comprend 3 unités, le compteur d'unités au sein du module de sécurité sera mis à jour cinq fois durant la communication et une cinquième fois en fin de communication.

Le procédé de gestion du compteur d'unités se définit par les étapes 10, 20, 30, 40, 50, 60 illustrées par la figure 2A.

Une étape préalable à l'enregistrement des unités consiste à vérifier l'état du compteur (étape 10) détaillée à partir de la figure 2B.

A chaque demande de mémorisation d'unités consommées, le système d'exploitation du module de sécurité gérant le compteur vérifie que le nombre de bits éteints (disponibles) dans la zone A est supérieur ou égal au nombre d'unités à mémoriser (cf. figure 2A).

Dans l'affirmative, si n unités ont été consommées, n bits disponibles dans la zone A sont grillés, (on peut prévoir à titre de variante selon l'application, que n bits disponibles dans la zone A soient grillés pour n paquets d'unités consommées).

Cette opération ne nécessite aucun effacement et seule une action d'écriture revient à griller certains bits de la zone A.

Dès que le nombre n d'unités consommées à mémoriser excède le nombre de bits disponibles L restant dans la zone A, on éteint le nombre de bits disponibles L dans la zone A et les unités consommées restantes n-L sont comptabilisées dans la zone B. Une nouvelle valeur codée tenant compte de ces unités restantes est

enregistrée dans la zone B par une opération de mise à jour comme suit :

La nouvelle valeur de la zone B (nombre total d'unités) est égale à la valeur courante de la zone B à laquelle il faut ajouter le nombre de bits grillés dans la zone A (valeur VA) et le nombre n-L d'unités à mémoriser.

La mise à jour de la zone B entraîne une lecture de celle-ci suivie d'un effacement et d'une écriture.

La zone A est quant à elle effacée entièrement (tous les bits sont de nouveau disponibles).

On pourrait prévoir également selon l'invention, dans le cas ou le nombre de bit disponibles dans la zone A est insuffisant, de compléter cette zone A, puis de faire une mise à jour de la zone B en mémorisant comme nouvelle valeur la valeur précédente à laquelle est ajouté le contenu de la zone A, puis d'effacer la zone A et enfin de mémoriser dans la zone A les unités consommées restantes (au lieu de les mémoriser dans la zone B). Cette variante reste bien dans le cadre du principe de l'invention.

Avec ce procédé, bien que la fréquence de mémorisation d'unités consommées soit importante, la fréquence d'effacement des zones A et B est bien plus faible. Il en est de même pour la fréquence d'écriture des différentes emplacements mémoire composant la zone A et par voie de conséquence la zone B.

La fréquence d'effacement et d'écriture des emplacements mémoire composant le compteur d'unités est directement liée d'une part à la dimension de la zone A et d'autre part à la granularité utilisée pour décomposer une communication (on entend par granularité une période élémentaire de communication correspondant à un nombre d'unités prédéterminé par l'opérateur).

On peut noter que pour connaître à tout instant le nombre total d'unités consommées à l'aide du publiphone, il suffit d'ajouter à la valeur courante de la zone B, le nombre de bits grillés de la zone A.

Dans le cadre de l'invention, il est proposé d'utiliser une fonctionnalité supplémentaire pour prolonger la durée de vie du compteur d'unités.

En effet, il est connu qu'un champ de bits est subdivisé en ensembles de huit bits consécutifs appelés octets. Comme il est décrit plus haut, la zone A est effacée aussi fréquemment que la zone B. Cependant, pour des facilités de programmation ou des contraintes liées au composant utilisé, le fait de griller un bit au sein d'un octet peut entraîner un nouveau grillage des bits déjà grillés au sein dudit octet.

Ainsi, un octet appartenant à la zone A peut être plus souvent écrit (c'est à dire, ses bits grillés) qu'un octet composant la zone B. La zone A étant alors plus stressée que la zone B, la durée d'exploitation du compteur est donc directement liée à la capacité de mémorisation de la zone A.

Pour pallier à ce problème, on propose dans le cadre de l'invention de prévoir au sein du compteur d'unités, une zone mémoire supplémentaire dénommée zone C comprenant au moins un emplacement pour mémoriser l'information C1 (cf. figure 1 et figure 5).

Cette variante du procédé est illustrée par la figure 5.

Dans cette variante, l'étape de vérification de l'état du compteur, préalable à l'enregistrement des unités consommées comporte une lecture de la zone C pour vérifier si l'information C1 existe.

Cette information C1 est écrite dès qu'un emplacement mémoire de la zone A ne peut plus être

effacé ou écrit (car il est prévu de manière classique de contrôler la bonne exécution d'une écriture ou d'un effacement de la mémoire). Dans ce cas le système d'exploitation du module de sécurité décide de désactiver la zone A (étape 42) et de ne travailler qu'avec la zone B (étape 80). A chaque demande de mémorisation d'unités consommées la zone B est effacée et réécrite.

Bien évidemment, la capacité de mémorisation de la zone B va à son tour rapidement être détériorée mais le compteur peut continuer à être exploité quelque temps encore.

D'autre part, pour renforcer la sécurité de la gestion du compteur, il est possible d'ajouter un mécanisme permettant de garantir un état cohérent dudit compteur, si une coupure de courant intervient durant l'opération de mémorisation. Il n'est pas pertinent d'envisager une opération d'arrachement du module de sécurité car généralement celui-ci est parfaitement intégré au publiphone. Ceci dit, le cas d'arrachement se gérerait de la même manière.

Dans le cadre de l'invention, pour implanter un tel mécanisme (appelé ci-après mécanisme de recouvrement), la zone B est dotée d'un code de redondance. De plus la zone B est dupliquée (cf. figure 1, 2B, et 3).

La zone SB ainsi définie est utilisée comme sauvegarde de la précédente. Elle est mise à jour avant toute modification de la zone B.

La zone SB contient à tout moment la valeur de la zone B, précédant la dernière mise à jour de la dite zone.

Un octet supplémentaire au sein de la zone C est utilisé pour indiquer si l'opération de mémorisation a

été partiellement ou entièrement effectuée, il s'agit de l'information témoin C2.

Ainsi, en début de traitement d'une demande de mémorisation d'unités, C2 est mémorisée. Elle est effacée une fois que cette même opération de mémorisation est entièrement réalisée. Pour éviter de trop stresser l'octet C2, celui-ci n'est utilisé (écrit puis effacé) que dans le cas où le nombre d'unités à mémoriser est supérieur au nombre de bits encore disponibles dans la zone A.

Dans le cas contraire, l'octet C2 est inutilisé. Parmi les bits disponibles de la zone A, n bits sont allumés. L'opération de mémorisation est terminée. On considère que la perte d'information est minime.

Dans le cas où le nombre de bits disponibles au sein de la zone A est insuffisant, il est impératif d'activer la procédure permettant ultérieurement d'actionner le mécanisme de recouvrement au cas où il y a anomalie.

En effet, si une coupure de courant survient après que la zone B ait été effacée et non à nouveau réécrite, toute l'information du compteur d'unités serait perdue.

On va maintenant détailler l'étape préalable à tout enregistrement de vérification du compteur (figure 2B).

Le système vérifie l'absence du témoin C2 (11).

Si le témoin C2 est absent (12), le système vérifie les champs contenant les codes de redondance.

Si ces champs sont valides (13) on enregistre les n unités consommées.

Si les champs ne sont pas valides (14), il y a détection d'un défaut, arrêt du compteur (et éventuellement une alarme).

Dans le cas ou le témoin existe (15) il y a mise en oeuvre du mécanisme de recouvrement détaillé à partir de la figure.

On va maintenant détailler l'opération de mise à jour de la zone B selon cette variante (cf figure 3).

Comme on peut le voir sur la figure 3 (étapes 51 à 55), le témoin C2 est tout d'abord écrit, la valeur courante par exemple V0 du compteur codée dans la zone B est recopiée dans la zone SB. Puis la zone B est mise à jour (nouvelle valeur V1 égale à la valeur courante à laquelle on ajoute le nombre de bits grillés dans la zone A et les n-L unités restantes à mémoriser). La zone A est ensuite effacée et le témoin C2 est alors effacé pour indiquer que l'opération de mémorisation a été effectuée entièrement avec succès.

Dans la description réalisée, tout se passe normalement, il n'y a pas eu coupure d'alimentation durant l'opération de mémorisation.

A présent, si une coupure est intervenue, l'activation du mécanisme de recouvrement est décrite ci-après (cf. figure 4).

Celui-ci est activé lors de la prochaine demande de mémorisation que le nombre de bits disponible au sein de la zone A soit suffisant ou non pour mémoriser les n unités.

Si le témoin C2 est allumé alors avant de mémoriser les unités consommées, le mécanisme de recouvrement est actionné par le système d'exploitation du module de sécurité.

Plusieurs cas se présentent. En effet la coupure a pu intervenir durant la mise à jour de la zone SB (cas 1), durant la mise à jour de la zone B (cas 2), durant l'effacement de la zone A (cas 3) ou entre ledites mises à jour (cas 4 et cas 5).

La procédure de recouvrement doit être distincte en fonction des différents cas listés précédemment.

Dans le cas où la zone SB n'a pu être correctement mise à jour (cas 1), le code de redondance SCR de celle-ci n'est pas conforme. La valeur contenue V0 dans la zone B est alors recopiée dans la zone SB, la zone B est ensuite mise à jour (nouvelle valeur V1 égale à la valeur courante V0 de la zone B à laquelle il faut ajouter le nombre de bits grillés dans la zone A valeur VA). Seul le nombre d'unités n-L qui devaient être mémorisé lors de la mémorisation interrompue est perdu.

La zone A est alors effacée et le témoin C2 également.

Dans le cas où la zone SB a été correctement mise à jour mais la zone B ne l'a pas été correctement (cas 2), le code de redondance SCR de la zone SB est correct. Par contre, celui CR de la zone B est incorrect.

La zone B est alors mise à jour comme suit :

La nouvelle valeur V1 de la zone B est égale à la valeur V0 de la zone SB à laquelle on ajoute le nombre de bits grillés dans la zone A c'est à dire une valeur VA, V1 = V0 + VA.

Dans ce cas comme dans le précédent, la seule information perdue correspond au nombre n-L unités restantes qui devait être mémorisé durant la mémorisation interrompue. La zone A est alors effacée et le témoin C2 également.

En examinant seulement les codes de redondance de la zone SB et de la zone B, il est impossible de savoir si la coupure de courant a eu lieu entre la mise à jour des zones SB et B (cas 4) ou après la mise à jour de ces deux zones (cas 5). En effet dans ces deux cas les codes de redondance sont tous les deux corrects.

Pour distinguer les cas 4 et 5, le système d'exploitation du module de sécurité compare les valeurs des zones SB et B : V(SB) = V(B) ? :

Si la zone SB contient la même valeur que la zone B alors la coupure d'alimentation a dû avoir lieu entre la mise à jour des zones SB et B (cas 4). Le traitement du mécanisme de recouvrement est alors identique à celui détaillé précédemment (cas 2).

Dans le cas contraire, la zone B a donc dû être correctement mise à jour (cas 5). Il faut alors effacer la zone A et le témoin C2. Aucune information n'a été perdue dans ce cas.

Il reste à traiter le cas où la coupure de courant a eu lieu durant l'effacement de la zone A (cas 3). Ce cas est similaire au cas précédent (cas 5).

Une fois que le mécanisme de recouvrement a été exécuté, les n unités à mémoriser le sont conformément à la description de l'invention réalisée précédemment.

REVENDICATIONS

1. Procédé de gestion sécurisée d'un compteur d'unités dans une mémoire programmable et effaçable électriquement, selon lequel on enregistre un nombre d'unités consommées par des utilisateurs au moyen du compteur, caractérisé en ce qu'il consiste à décomposer le compteur d'unités en au moins deux zones mémoires (A, B), une première zone (A) dans laquelle on mémorise au moins un bit par au moins une unité consommée et une deuxième zone (B) dans laquelle on mémorise la valeur correspondant au cumul d'unités consommées, la deuxième zone n'étant mise à jour que lorsque le nombre d'unités consommées dépasse ou atteint le nombre de bits non mémorisé dans la première zone.

2. Procédé de gestion d'un compteur selon la revendication 1, caractérisé en ce que les unités consommées sont enregistrées dans la première zone de manière cyclique.

3. Procédé de gestion selon les revendications 1 et 2, caractérisé en ce qu'une opération d'enregistrement de n unités consommées comprend les étapes suivantes :

- lecture du contenu de la première zone (A) et comparaison du nombre de bits (L) non mémorisés de la zone (A) au nombre d'unités (n) consommées à enregistrer,
- si ce nombre de bits non mémorisés (L) est supérieur ou égal au nombre d'unités (n) à enregistrer, on mémorise les (n) bits correspondant dans ladite zone (A),

- si ce nombre (L) est inférieur, on mémorise (L) bits dans la première zone (A) et on enregistre les (n-L) unités restantes dans la deuxième zone (B) en effectuant une opération de mise à jour de cette zone et la première zone (A) est effacée.

4. Procédé de gestion selon l'une quelconque des revendications 1 à 4 caractérisé en ce qu'une opération de mise à jour de la deuxième zone (B) comprend une étape d'écriture dans cette zone d'une nouvelle valeur de compteur codée égale à la valeur courante à laquelle on ajoute le nombre de bits mémorisés de la première zone (A) et les (n-L) unités restantes consommées à mémoriser.

5. Procédé de gestion selon la revendication 4 caractérisé en ce que la mise à jour comprend une étape préalable d'enregistrement d'une information témoin (C2) signifiant qu'une mise à jour est en cours.

6. Procédé de gestion selon l'une quelconque des revendications précédentes caractérisé en ce que le compteur d'unité comporte une zone de sauvegarde (SB) de la deuxième zone (B) et en ce que ces deux zones comportent chacune un champs pour l'enregistrement d'un code de redondance (CR, SCR) pour la vérification de l'intégrité du contenu de ces deux zones.

7. Procédé de gestion selon les revendications 4 et 5, caractérisé en ce qu'une opération d'enregistrement de n unités consommées comprend en outre une étape préalable de vérification de l'état du compteur comprenant les opérations suivantes :

- vérification de l'absence de l'information témoin d'une mise à jour en cours :
  - dans le cas où l'information témoin est bien absente :
    - vérification de la validité des champs contenant les codes de redondances :
      . dans le cas où les champs sont valides :
        - enregistrement des n unités;
      . dans le cas où les champs ne sont pas valides :
        - détection d'un défaut et arrêt du compteur.
  - dans le cas où l'information témoin est présente :
    - activation de l'opération de recouvrement pour rétablir l'intégrité des contenus du compteur.

8. Procédé de gestion selon les revendications 6 et 7, caractérisé en ce qu'une opération de mise à jour de la deuxième zone (B) comporte alors les étapes suivantes:
- enregistrement de l' information témoin (C2),
- recopie dans la zone de sauvegarde (SB) de la valeur (V0) du compteur codée de la deuxième zone (B),
- enregistrement de la nouvelle valeur du compteur codée dans la deuxième zone (B),
- effacement de l'information témoin (C2),

9. Procédé de gestion selon la revendication 8, caractérisé en ce que l'opération de recouvrement consiste à déterminer à quelle étape s'est produite l'anomalie, puis à opérer selon le cas déterminé, les étapes de mise à jour de la zone de sauvegarde (SB)

et/ou de la deuxième zone (B) et/ou de la première zone (A).

10. Procédé de gestion selon la revendication 9, caractérisé en ce que la détermination de l'étape à laquelle s'est produite l'anomalie consiste à lire le contenu de chacune des zones pour savoir si l'anomalie s'est produite pendant la mise à jour de la zone de sauvegarde (SB) cas 1, pendant la mise à jour de la deuxième zone (B) cas 2, pendant l'effacement de la première zone (A) cas 3, entre la mise à jour de la deuxième zone (B) et la zone de sauvegarde (SB) cas 4, après la mise à jour de ces deux zones cas 5,

. dans le cas 1 à :

- recopier la valeur contenue dans la deuxième zone (B) dans la zone de sauvegarde (SB),
- mettre à jour la deuxième zone (B) en enregistrant la nouvelle valeur qui est égale à l'ancienne à laquelle on ajoute le contenu de la première zone (A),
- effacer la première zone (A),
- effacer l'information témoin (C2) ;

. dans le cas 2 à :

- recopier dans la deuxième zone (B) la valeur contenue dans la zone de sauvegarde (SB) en rajoutant la valeur contenue dans la première zone (A),
- effacer la première zone (A),
- effacer l'information témoin (C2) ;

. dans le cas 3 à :

- effacer le contenu de la première zone (A),
- effacer l'information témoin (C2) ;

. dans le cas 4 à :

- mettre en oeuvre les étapes selon le cas 2 ;

. dans le cas 5 à :

- mettre en oeuvre les étapes selon le cas 3.

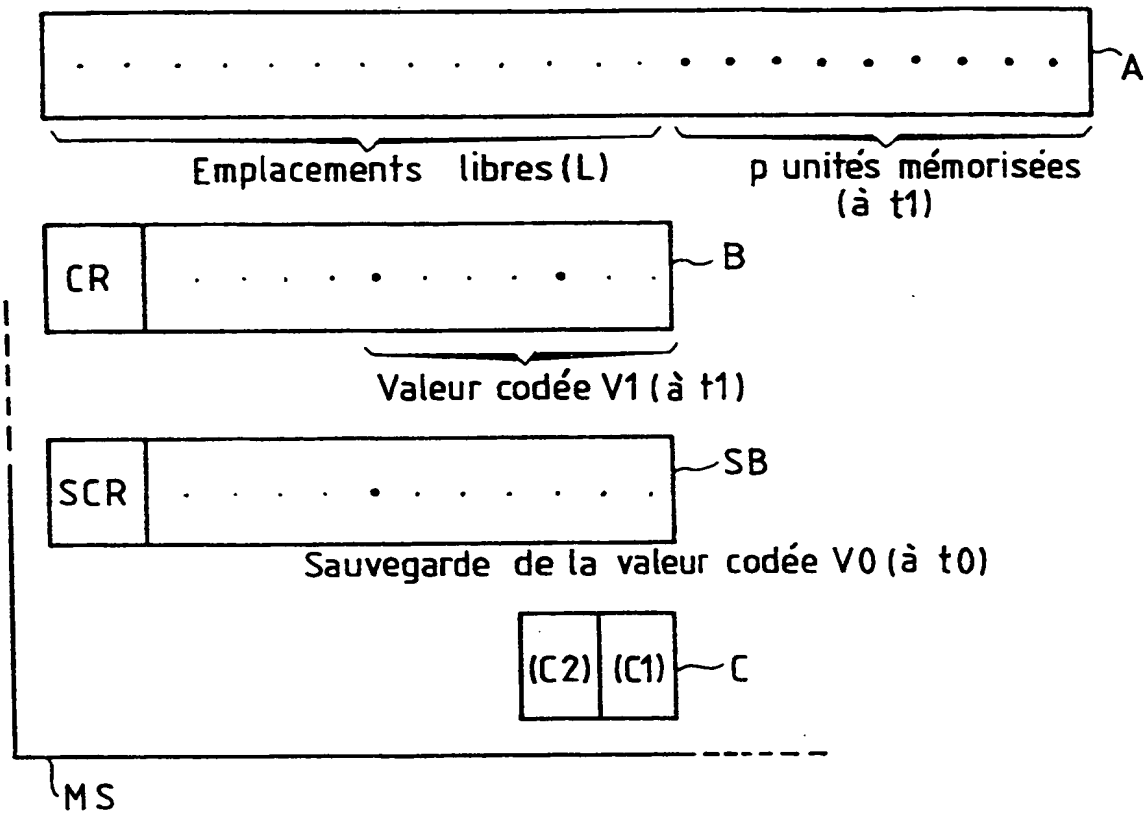
11. Procédé de gestion selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend l'étape d'enregistrement d'une information significative (C1) d'une défaillance en lecture ou en écriture de la première zone (A) désactivant ladite zone lorsqu'il n'a pas été possible de lire ou d'écrire dans cette zone, une étape de lecture de cette information à chaque nouveau cycle, les unités consommées étant alors directement enregistrées de manière codée par une opération de mise à jour de la deuxième zone (B).

12. Procédé de gestion selon la revendication 5 et la revendication 11, caractérisé en ce que l'information témoin (C2) d'une mise à jour en cours et l'information significative d'une défaillance (C1) en lecture et en écriture de la première zone sont enregistrées dans une troisième zone (C) dudit compteur.

13. Module de sécurité (MS) mettant en oeuvre le procédé selon l'une quelconques des revendications précédentes.

14. Module de sécurité selon la revendication 13, caractérisé en ce qu'il est implanté dans un terminal gérant des unités consommées, notamment un terminal de téléphonie.

FIG_1


A
Emplacements libres (L)
p unités mémorisées (à t1)
CR
B
Valeur codée V1 (à t1)
SCR
SB
Sauvegarde de la valeur codée V0 (à t0)
(C2)
(C1)
C
MS

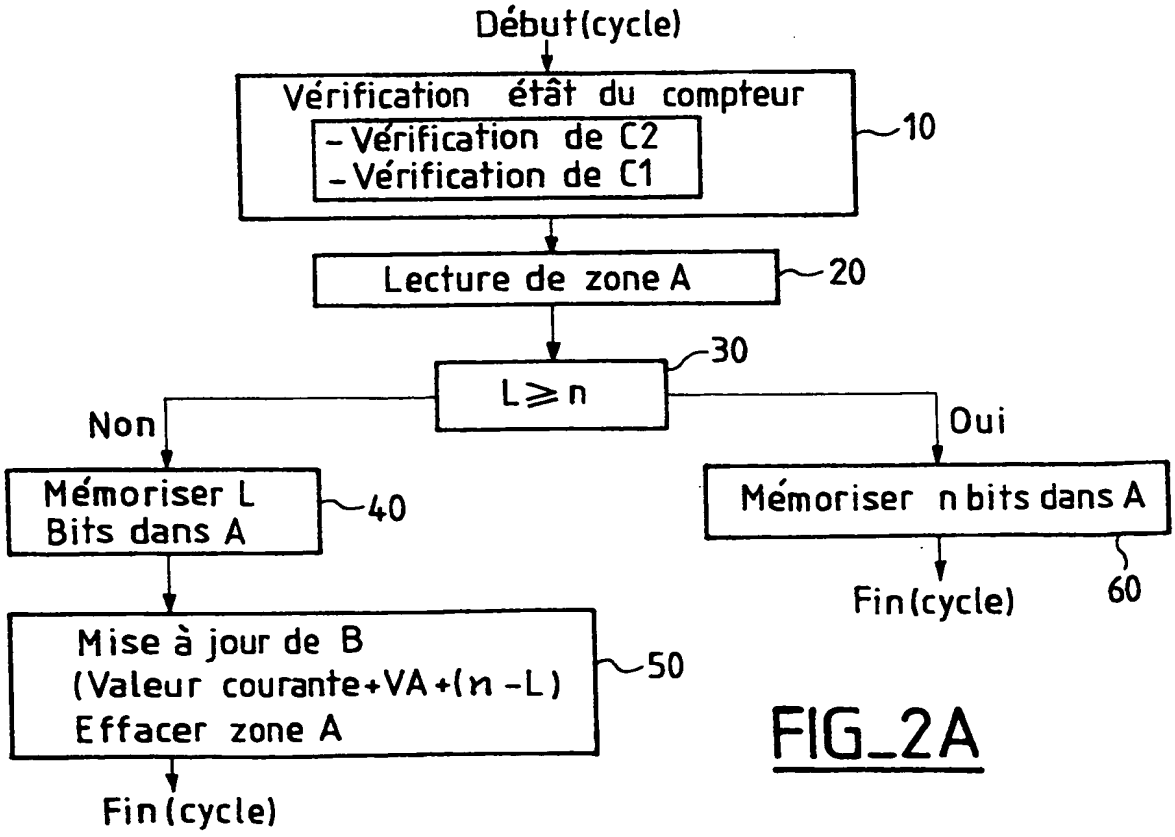

Début (cycle)
Vérification état du compteur
- Vérification de C2
- Vérification de C1
10
Lecture de zone A
20
L ≥ n
30
Non
Oui
Mémoriser L Bits dans A
40
Mémoriser n bits dans A
Fin (cycle)
60
Mise à jour de B
(Valeur courante + VA + (n - L)
Effacer zone A
50
Fin (cycle)

FIG_2A

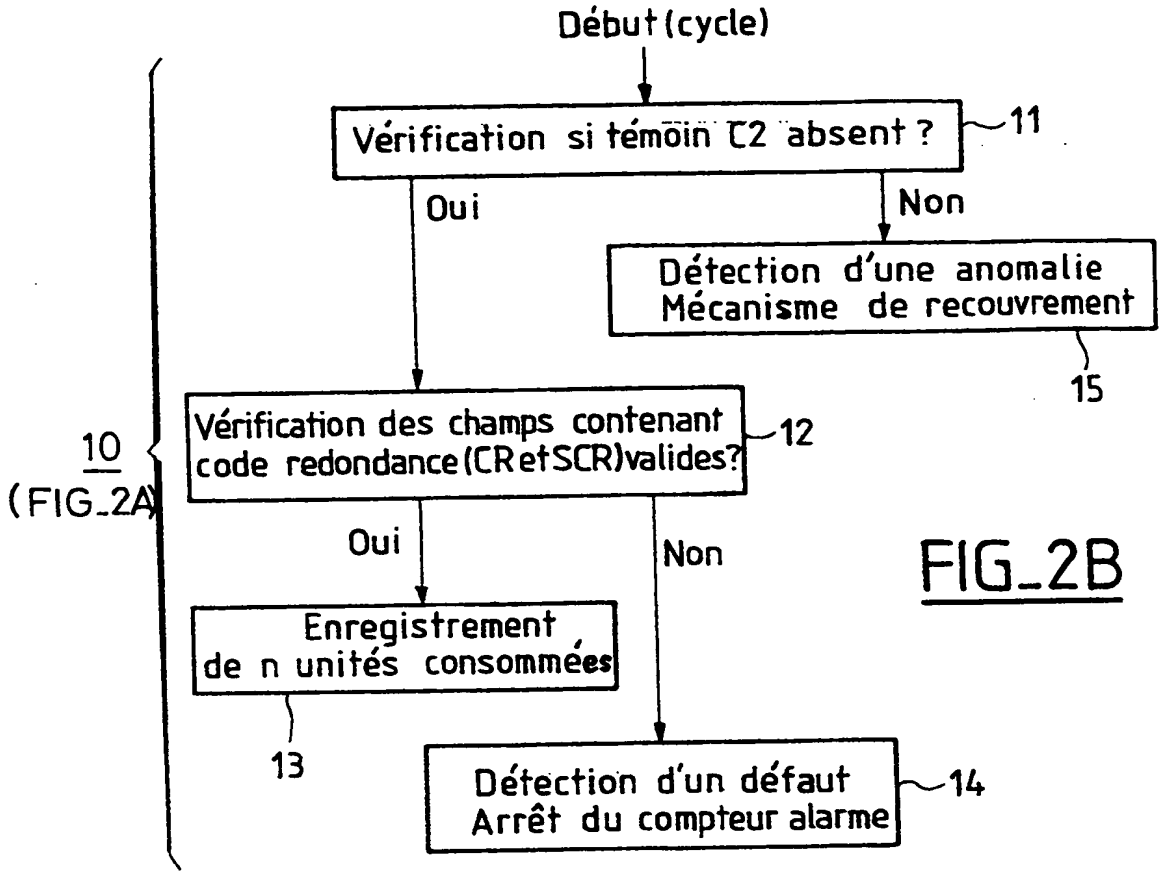
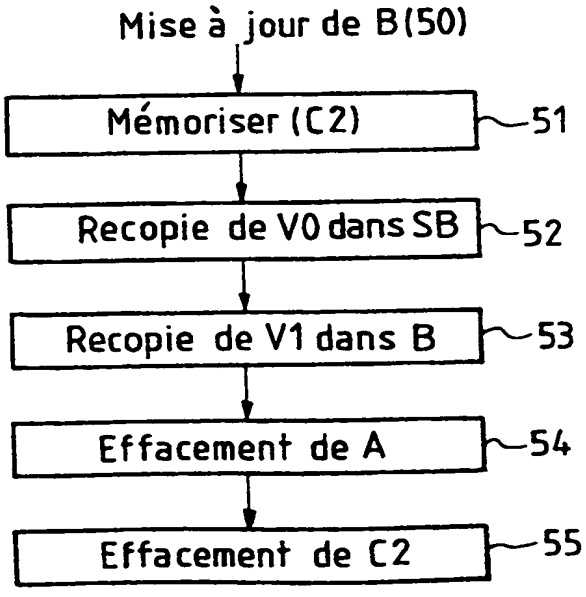

Début (cycle)
Vérification si témoin C2 absent ?
11
Oui
Non
Détection d'une anomalie
Mécanisme de recouvrement
15
Vérification des champs contenant
code redondance (CR et SCR) valides?
12
10
(FIG_2A)
Oui
Non
Enregistrement
de n unités consommées
13
Détection d'un défaut
Arrêt du compteur alarme
14

FIG_2B

FIG_3


Mise à jour de B (50)
Mémoriser (C2)
51
Recopie de V0 dans SB
52
Recopie de V1 dans B
53
Effacement de A
54
Effacement de C2
55

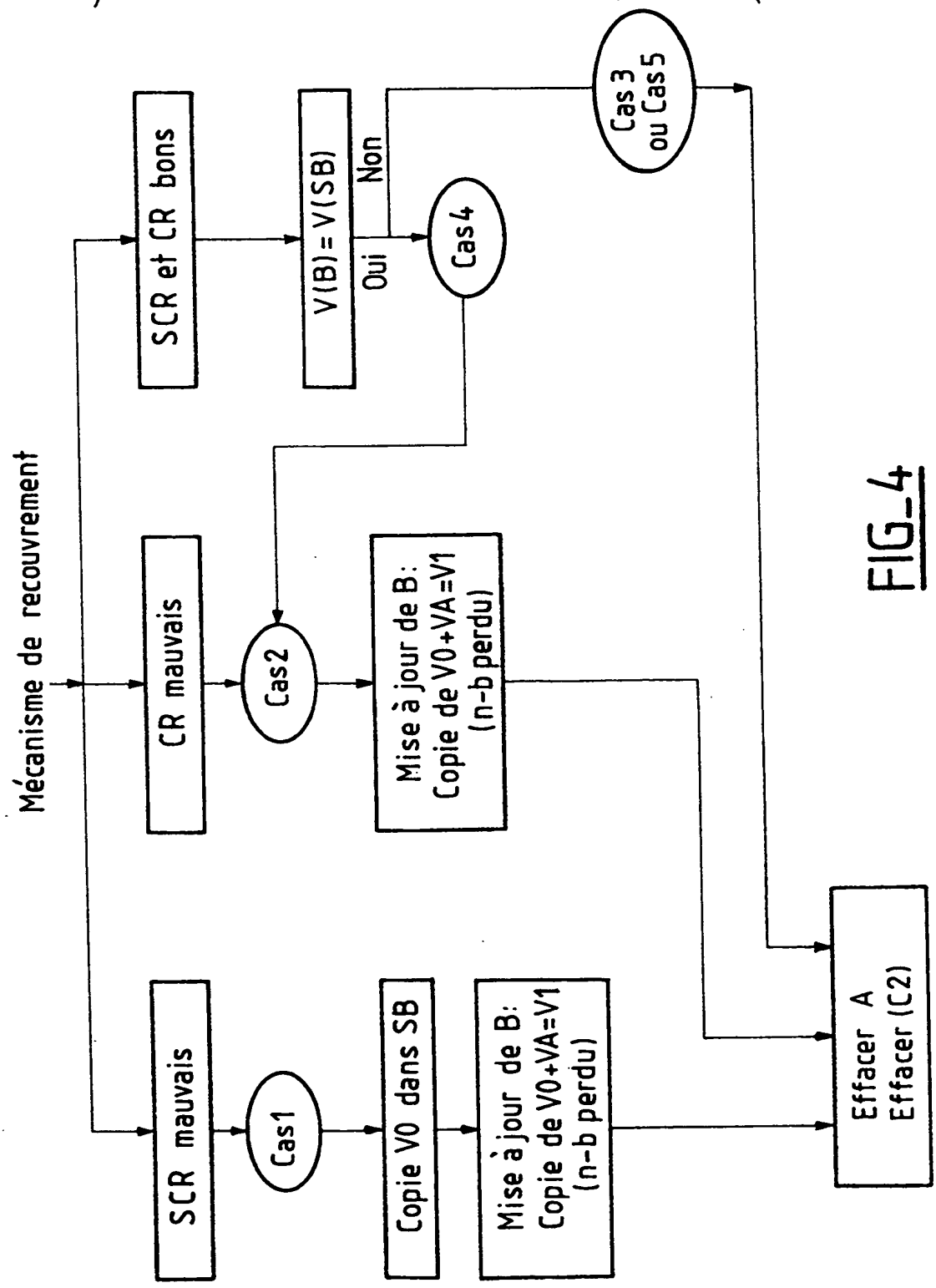
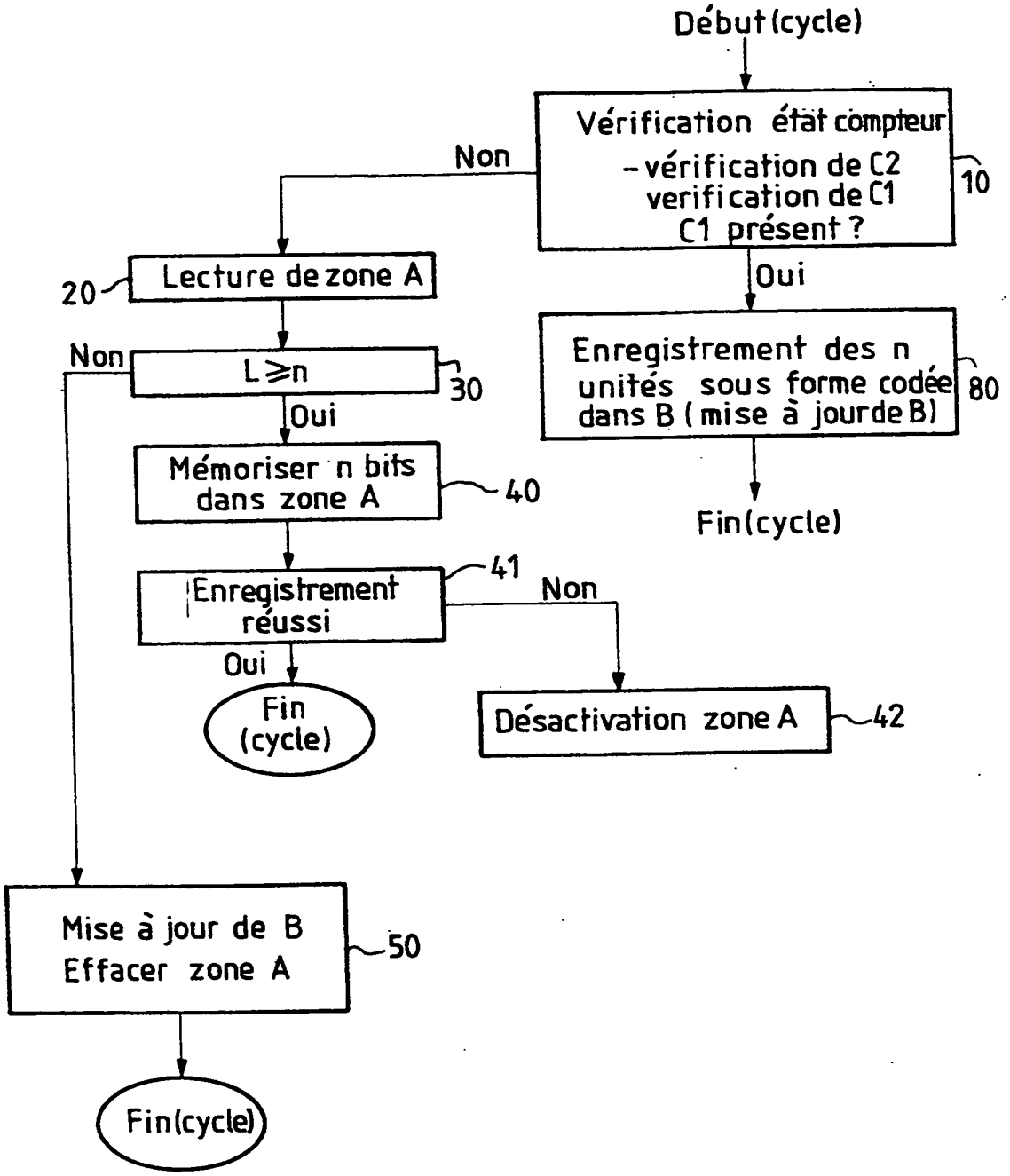

15
(FIG_2B
Mécanisme de recouvrement
SCR et CR bons
V(B) = V(SB)
Oui
Non
Cas 3
ou Cas 5
Cas4
CR mauvais
Cas2
Mise à jour de B:
Copie de V0+VA=V1
(n-b perdu)
SCR mauvais
Cas1
Copie V0 dans SB
Mise à jour de B:
Copie de V0+VA=V1
(n-b perdu)
Effacer A
Effacer (C2)

FIG_4

FIG_5


Début (cycle)
Vérification état compteur
- vérification de C2
verification de C1
C1 présent ?
10
Non
Oui
20
Lecture de zone A
Non
L ⩾ n
30
Oui
Mémoriser n bits
dans zone A
40
Enregistrement des n
unités sous forme codée
dans B (mise à jour de B)
80
Fin (cycle)
Enregistrement
réussi
41
Non
Oui
Fin
(cycle)
Désactivation zone A
42
Mise à jour de B
Effacer zone A
50
Fin (cycle)

INTERNATIONAL SEARCH REPORT

In [redacted] Application No
PCT/FR 99/00292

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04M17/00 H04M17/02 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04M G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 626 664 A (GEMPLUS CARD INT) 30 November 1994 see column 1, line 54 - column 2, line 11 see claim 1 ---	1-14
A	EP 0 781 065 A (ALCATEL MOBILE COMM FRANCE) 25 June 1997 see abstract ---	1-14
A	US 4 887 234 A (IIJIMA YASUO) 12 December 1989 see the whole document ---	1-14
A	EP 0 368 752 A (BULL CP8) 16 May 1990 see the whole document -----	1-14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 March 1999	26/03/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Montalbano, F

1

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 99/00292

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0626664 A	30-11-1994	FR 2704704 A	04-11-1994
		DE 69400549 D	24-10-1996
		DE 69400549 T	30-01-1997
		ES 2092867 T	01-12-1996
		JP 7073281 A	17-03-1995
		SG 48143 A	17-04-1998
		US 5687398 A	11-11-1997
EP 0781065 A	25-06-1997	FR 2742959 A	27-06-1997
		AU 7414796 A	26-06-1997
		CA 2193712 A	22-06-1997
		JP 9187081 A	15-07-1997
US 4887234 A	12-12-1989	JP 62159295 A	15-07-1987
		JP 62128388 A	10-06-1987
		JP 62128390 A	10-06-1987
		DE 3635409 A	04-06-1987
		FR 2591008 A	05-06-1987
EP 0368752 A	16-05-1990	FR 2638868 A	11-05-1990
		AT 164249 T	15-04-1998
		CA 2002349 A,C	09-05-1990
		DE 68928608 D	23-04-1998
		DE 68928608 T	16-07-1998
		DK 165390 A	22-08-1990
		ES 2114852 T	16-06-1998
		WO 9005347 A	17-05-1990
		JP 7048178 B	24-05-1995
		JP 3500827 T	21-02-1991
		NO 300438 B	26-05-1997
		US 5434999 A	18-07-1995

RAPPORT DE RECHERCHE INTERNATIONALE

De[illegible]rnationale No
PCT/FR 99/00292

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 H04M17/00 H04M17/02 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 H04M G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 626 664 A (GEMPLUS CARD INT) 30 novembre 1994 voir colonne 1, ligne 54 - colonne 2, ligne 11 voir revendication 1 ---	1-14
A	EP 0 781 065 A (ALCATEL MOBILE COMM FRANCE) 25 juin 1997 voir abrégé ---	1-14
A	US 4 887 234 A (IIJIMA YASUO) 12 décembre 1989 voir le document en entier ---	1-14
A	EP 0 368 752 A (BULL CP8) 16 mai 1990 voir le document en entier -----	1-14

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
18 mars 1999	26/03/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Montalbano, F

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 99/00292

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0626664 A	30-11-1994	FR 2704704 A	04-11-1994
		DE 69400549 D	24-10-1996
		DE 69400549 T	30-01-1997
		ES 2092867 T	01-12-1996
		JP 7073281 A	17-03-1995
		SG 48143 A	17-04-1998
		US 5687398 A	11-11-1997
EP 0781065 A	25-06-1997	FR 2742959 A	27-06-1997
		AU 7414796 A	26-06-1997
		CA 2193712 A	22-06-1997
		JP 9187081 A	15-07-1997
US 4887234 A	12-12-1989	JP 62159295 A	15-07-1987
		JP 62128388 A	10-06-1987
		JP 62128390 A	10-06-1987
		DE 3635409 A	04-06-1987
		FR 2591008 A	05-06-1987
EP 0368752 A	16-05-1990	FR 2638868 A	11-05-1990
		AT 164249 T	15-04-1998
		CA 2002349 A,C	09-05-1990
		DE 68928608 D	23-04-1998
		DE 68928608 T	16-07-1998
		DK 165390 A	22-08-1990
		ES 2114852 T	16-06-1998
		WO 9005347 A	17-05-1990
		JP 7048178 B	24-05-1995
		JP 3500827 T	21-02-1991
		NO 300438 B	26-05-1997
		US 5434999 A	18-07-1995